Discussion.

The table below summarizes the seven distinct searches and examinations by the United States Patent and Trademark Office to which the claims remaining in this Application have been subjected and the three occasions on which the substance of the three claims remaining in this Application have been allowed:

Date	Action
1998-08-21	International Filing Date for PCT application (from which the current application flows) which included the essence of the claims remaining in this application in claims 153 to 158.
1998-12-17	**First Search**. International Search Report prepared by the United States Patent and Trademark Office showed no references of significance greater than "A" (general state of the art).
1999-04-06	**First Examination and First Allowance**. International Preliminary Examination Report prepared by the United States Patent and Trademark Office finding all 168 claims patentable, including Claims 153 to 157.
2001-02-09	**Second Allowance**. Office action allowing claims 153 to 157.
2001-10-10	Office action requiring an election and restriction for claims 153-158
2001-11-05	Current application filed electronically
2004-07-20	**Second Search and Second Examination**. Office Action denying all claims based upon prior art never before cited by the United States patent and Trademark Office
2005-06-15	**Third Search and Third Examination**. Office Action denying all claims based upon new prior art never before cited by the United States Patent and Trademark Office
2006-03-20	**Fourth Search and Fourth Examination**. Office Action denying all claims based upon new prior art never before cited by the United States Patent and Trademark Office
2007-01-22	**Third Allowance.** Office Action (i) concluding that Claim 3 would be allowable if rewritten in independent form and (ii) allowing Claims 10 and 11.
2007-07-17	Claim 3 amended as suggested by the examiner and all claims other

Date	Action
	than 3, 10 and 11 deleted.
2007-08-21	**Fifth Search and Fifth Examination**. Office Action denying all claims based upon new prior art never before cited by the United States Patent and Trademark Office
2008-09-22	Appeal brief filed.
2009-01-23	**Sixth Search and Sixth Examination**. Office Action denying all claims based upon new prior art never before cited by the United States Patent and Trademark Office.

If, after reviewing this response, the Examiner once again is persuaded that the prior art already cited by the Examiner does not justify rejecting the claims remaining in this Application, then the Applicant respectfully requests that the Examiner allow the pending claims (for the fourth time) and not perform a seventh search and seventh examination of the claims in this Application.

In this connection, Applicant respectfully draws the Examiners attention to MPEP Section 707.07(g) which discourages piecemeal examination.

(i) Real Party In Interest

The real party in interest is Grenex Corporation, the assignee.

(ii) Related Appeals And Interferences

There are no appeals or interferences known to Applicant, Applicant's legal representative or Applicant's assignee which will directly affect or be directly affected by or have a bearing on the subject matter of this response.

(iii) Status of Calims

The status of all the claims in this application is as follows:

Claims	Status
1	Canceled
2	Cancelled
3	Rejected
4	Cancelled
5	Cancelled
6	Cancelled
7	Cancelled
8	Cancelled

Claims	Status
9	Cancelled
10	Rejected
11	Rejected

Applicant respectfully requests reconsideration of the patentability of Claims 3, 10 and 11 for the reasons discussed below.

(iv) Status Of Amendments

No amendment has been filed subsequent to the Office Action.

(v) Summary Of Claimed Subject Matter

It is noted that this application was filed electronically, and not on paper. The electronic patent application as filed, and as contained in appellant's official electronic file, did not have and does not have page breaks or page numbers and instead only had and has paragraph numbers. Thus it is impossible to point to particular page numbers or line numbers on pages in any unambiguous way in the application as originally filed electronically.

After receiving the electronic patent application, USPTO personnel hand-printed it on paper, and inserted the printed paper into the workflow of the USPTO as if the application had been filed on paper (which it was not). USPTO's hand-printing imposed artificial page breaks bearing no relation to the document in applicant's files. The artificial page breaks may be seen in the IFW (image file wrapper) system, yielding forty-six pages.

Thus to avoid possible confusion, citations to the application herein are not only to the paragraph numbers in the patent application as originally filed, but also to the page numbers which were artificially imposed by the USPTO personnel after the application was filed (and to the "line numbers" based upon the page breaks artificially imposed by USPTO personnel after filing).

It is emphasized that the citations below to page and line numbers in no way constitute an admission that the application was filed on paper (which it was not) and in no way constitute an admission that the application as filed had page numbers at all (which it did not).

The invention relates generally to using tcp/ip port 80 (the default port for HTTP communication) for HTTPS communication, thereby enabling secure HTTPS communication through firewalls that permit access to port 80, but block access to port 443 (the default port for HTTPS communication). See the Specification at paragraphs 230 to 0246, page 30, line 6 to page 32, line 9.

NOTE: In this Application as currently amended, Applicant NEITHER claims the broad concept of changing the port number used for HTTPS communication NOR claims the broad concept of using HTTPS to perform secure communication. Rather, in this Application as currently amended, Applicant merely claims the relatively narrow improvement of using port 80 in particular (which is normally associated with HTTP communication) for HTTPS communication.

In a **first** embodiment (i.e., claim 3) the invention includes:

(a) configuring a server program so that it listens on port 80 for requests for secure hypertext transfer protocol sessions (rather than on port 443); (see the Specification at Paragraphs 234 to 240, page 30, line 24 to page 31, line 21); in a preferred embodiment, Internet Information Server is configured to use port 80 for HTTPS connections;

(b) receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443; (see the Specification at Paragraph 241, page 31, lines 22-24, and Claims 1 and 3); in a preferred embodiment, a browser requests a URL of the form "https://<address>:80" and that request is received by the server; and

(c) outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443; (see the Specification at Paragraph 241, page 31, lines 22-24, and Claims 1 and 3);

In a **second** embodiment (i.e., claim 10) the invention includes:

(a) configuring a web server system to use port 80 for communications using a protocol selected from the group consisting of: secure socket layer, secure sockets layer, SSL, secure hypertext transfer protocol, and HTTPS; (see the Specification at Paragraphs 234 to 240, page 30, line 24 to page 31, line 21);

(b) receiving at port 80 at the web server system a first data packet that is formatted in accordance with the protocol; (see the Specification at Paragraph 241, page 31, lines 22-24, and Claim 10); and

(c) responding to the first data packet with a second data packet that is formatted in accordance with the protocol. (See the Specification at Paragraph 241, page 31, lines 22-24, and Claim 10.)

In a **third** embodiment (i.e., claim 11) the invention includes a web server system comprising:

(a) web server software configured to use port 80 for communications using a protocol selected from the group consisting of: secure socket layer, secure sockets layer, SSL, secure hypertext transfer protocol, and HTTPS; (see the Specification at Paragraphs 234 to 240, page 30, line 24 to page 31, line 21, and Claim 11);

(b) means for receiving at port 80 at the web server system a first data packet that is formatted in accordance with the protocol (see the Specification at Paragraphs 234 to 240, page 30, line 24 to page 31, line 21 - Internet Information Server configured as described therein is such a means); and

(c) means for responding to the first data packet with a second data packet that is formatted in accordance with the protocol; (see the Specification at Paragraphs 234 to 240, page 30, line 24 to page 31, line 21 - Internet Information Server configured as described therein is such a means).

(vi) Grounds of rejection addressed in this response.

The **first** ground of rejection addressed in this response is the rejection of Claim 3 under 35 U.S.C. 103(a) as being unpatentable over Cianfrocca (US Patent No. 6,088,796) and further in view of Ogden et al (US Patent No. 6,161,137).

The **second** ground of rejection addressed in this response is the rejection of Claim 10 under 35 U.S.C. 103(a) as being unpatentable over Cianfrocca and further in view of Ogden.

The **third** ground of rejection addressed in this response is the rejection of Claim 11 under 35 U.S.C. 103(a) as being unpatentable over Cianfrocca and further in view of Ogden.

(vii) Discussion

Discussion - Claim 3

3. Claim 3 IS patentable over Cianfrocca further in view of Ogden because:

3.1. None of Cianfrocca, Ogden, nor Cianfrocca combined with Ogden, teaches or even suggests: configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

3.1.1. Cianfrocca alone does NOT teach or even suggest configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

3.1.1.1. In the Office action at page 3 lines 15 - 19, the Examiner (i) asserts that "Cianfrocca et al. disclose a method for securely communicating with a server program using a secure hypertext transfer protocol which by default uses a first port number associated therewith, said method practiced in connection with a hypertext transfer protocol which defaults to the use of a second port number associated therewith [col. 17, lines 35-40] ..."

The lines in Cianfrocca cited by the Examiner (i.e., col. 17, lines 35-40) actually say "Web browsers accessing the system from outside the DMZ will connect via HTTP/HTTPS on the normal TCP ports for these protocols (80 and 443, respectively), so the messenger system must be configured to allow these connections, and to disallow TMSP connections on ports 80 and 443".

Thus the disclosure in Cianfrocca cited by the Examiner expressly teaches AWAY from the requirements of Claim 3 because Cianfrocca at col. 17, lines 35-40 expressly teaches that the server should be configured to listen for requests for secure hypertext transfer protocol sessions on port 443 (NOT port 80 as required by Claim 3).

Cianfrocca at col. 17 lines 35-40 is discussing Cianfrocca's FIG. 4. Presumably then, the Examiner takes the position that the "Web Server Running Messenger System" shown inside the DMZ in Cianfrocca's FIG. 4 corresponds to the server on which the server program of Claim 3 runs.

The only secure hypertext transfer protocol disclosed by Cianfrocca at col. 17 lines 35-40 is HTTPS. Presumably then, the Examiner takes the

position that HTTPS (as disclosed by Cianfrocca) corresponds to the secure hypertext transfer protocol required by claim 3.

The only port that Cianfrocca at col. 17 lines 35-40 discloses for HTTPS is the normal TCP port of 443. Presumably then, the Examiner takes the position that port 443 in Cianfrocca corresponds to the first port number of Claim 3. This is not surprising, since Claim 3 expressly states that the first port number is 443.

The second hypertext transfer protocol disclosed by Cianfrocca in col. 17, lines 35-40 is HTTP. Presumably then, the Examiner takes the position that HTTP (as disclosed by Cianfrocca) corresponds to the hypertext transfer protocol of Claim 3.

The only port that Cianfrocca at col. 17 lines 35-40 discloses for HTTP is port 80. Presumably then, the Examiner takes the position that port 80 (as disclosed by Cianfrocca) corresponds to the second port of Claim 3. This is not surprising, since Claim 3 expressly states that the second port number is 80.

3.1.1.2. In the Office Action at page 3, lines 20-23, the Examiner asserts "... said method comprising: (a) configuring the server program so that it listens for requests for secure hypertext transfer protocol sessions [col. 14, line 57 to col. 15, line 32; Fig 4];"

Applicant concedes that Cianfrocca at Col. 14, line 57 to col. 15, line 32 discloses configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions. Applicant also concedes that Cianfrocca at Fig. 4 discloses forwarding session requests addressed to ports 80 and 443 to a server.

3.1.1.3. In the Office Action at page 4, lines 8-9 the Examiner asserts "Cianfrocca et al. further disclose wherein the first port number is 443 and the second port number is 80 [col. 17, lines 35-40] ...".

However, Cianfrocca at col. 17, lines 35-40 expressly teaches that the server should be configured to listen for requests for secure hypertext transfer protocol sessions on port 443 (NOT port 80 as required by Claim 3).

3.1.1.4. In the Office Action at page 4, lines 9-12 the Examiner asserts that Cianfrocca further disclose that "... it is possible to change the port

for one specific protocol connection providing that no other process is already listening and to specify one port for both types of protocol connections [col. 15, lines 28-32 and 40-42]."

Cianfrocca at col. 15, lines 28-32 actually says "To do so, HTTP connections on some particular port are allowed. This will typically be port 80, the IANA-standard port for HTTP connections, but it can be any value selected, provided no other process is already listening on that port." Nothing in the foregoing discloses anything about changing the port used for HTTPS communications. Claim 3 requires using a non-default port for HTTPS connections.

Cianfrocca at col. 15, lines 40-42 actually says "In this example, it is possible to specify a single TCP port to accept both the HTTP connections from the browsers and the TMSP connections from the application server." Cianfrocca at col. 14, lines 56-57 discloses that TMSP is "... a full-duplex protocol derived from HTTP." Consequently, TMSP has no obvious connection to HTTPS. Nothing in Cianfrocca at col. 15, lines 40-42 discloses anything about changing the port used for HTTPS communications. Claim 3 requires using a non-default port for HTTPS connections.

Cianfrocca Conclusion. Thus, for the reasons discussed above, Cianfrocca alone neither teaches nor suggests configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443, despite the Examiner's assertions to the contrary.

3.1.2. Ogdon alone does NOT teach or even suggest configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443. In the Office action at page 4 lines 13-18, the Examiner asserts that "Ogdon teaches the second port, port 80, rather than the first port, port 443, can be used for communication with the server using the secure hypertext transfer protocol, which is one of the various protocols selected from the group consisting of: secure socket layer, secure sockets layer, SSL, secure hypertext transfer protocol, and HTTPS [col. 16 lines 14-31].

Applicant finds this assertion by the Examiner particularly confusing. It is essentially the same as the assertion that the Examiner made in the Office

Action mailed August 21, 2007at page 3 lines 7-9. That assertion was the subject of Paragraph 3.1.2 of the Appeal Brief filed on 09/22/2008. In the current Office Action at page 2, lines 4-9, the Examiner said he was persuaded by Applicant's argument in the Appeal Brief filed on 09/22/2008 that Ogdon does NOT teach or even suggest configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

Applicant is at a loss to understand how the Examiner went from persuaded to un-persuaded within 3 double spaced pages.

In hopes that the Examiner can be re-persuaded, here again are the arguments on this point that were set forth in the Appeal Brief filed on 09/22/2008.

The cited lines in Ogdon do at least contain several relevant words (e.g., "security", "port numbers", "80", "servers", "HTTPS", "Secure Sockets Protocol"), but in those lines they are not connected together in a way that is relevant to this Application. To best understand what Ogdon teaches in the lines cited by the examiner, one should find the box labeled "Security Sub-System 208" in the middle of Fig. 1.A and read straight through Ogdons discussion of security from col. 14 line 27 to col. 18 line 19, rather than peeking through the keyhole suggested by the Examiner.

Ogdon's discussion of the Security Sub-System begins at Col. 14 lines 37 to 40 (not cited by the examiner) with the following:

> "Each host 200 is also in communication with the security subsystem 208 referred to hereinabove. Note that all external communications from third parties to a host 200 is [sic.] routed through the security subsystem 208."

At col. 14 lines 40 to 63, Ogdon describes various measures that might be employed by the Security Sub-System, including: packet filtering routers, firewalls, encryption tunnels, a validation subsystem and virus detection software.

At col. 14 line 64 to col. 15 line 2, Ogdon notes that security subsystem 208 resides on a separate computational host and may translate packets received from the network (e.g., Internet) to proprietary formats before forwarding them to other elements of Ogdon's system.

At col. 15 lines 2 to 15, Ogdon discusses how security can be weak for some presentations and strong for other presentations.

At col. 15 lines 16 to 27, Ogdon notes that the distributed content server features of Ogdon's system permit proprietary corporate data to reside behind the proprietary corporate firewall where it is unavailable even to Ogdon's system operators.

At col. 15 lines 28 to 66, Ogdon describes some of the ways in which security can vary from minimal to high.

At col. 15 line 66 to col. 16 line 3 (not cited by the Examiner), Ogdon observes that:

> "Furthermore, the high security measures may only allow network 70 connections from pre-approved network addresses using a specified protocol and port number for the duration of a particular presentation for which the client is registered."

The description of Ogdon's Security Subsystem summarized above, and the sentence quoted immediately above, make it clear that Ogdon teaches using non-standard port numbers as a means to achieve "security through obscurity". I.e., if someone with low personal moral standards who is not authorized to receive a highly secured presentation tries to view it any way by requesting information through standard port numbers, such would-be miscreant will be frustrated because the information will actually be available only through non-standard port numbers and then only if he is using a computer with a pre-approved IP address.

Ogdon at col. 16 lines 4-7 mentions that presentation data can be encrypted when it is sent over the Internet.

Ogdon at col. 16 lines 7-14 seems to be saying that if certain assumptions are satisfied, then a "presentation can implement standard web data security by using Internet protocols such as file transfer protocol (FTP) with user identification plus password, and hypertext transport protocol secure (HTTP)"

Turning now to the lines in Ogdon cited by the Examiner, and taking them one sentence at a time:

Ogdon at col. 16 lines 14-19 says:

"Also note that the security measures for the present invention are not restricted to providing communications on generally used port numbers (e.g., communication between the host and leaders or audience members can occur on either port 60 or port 80 in any combination for a single presentation performance[])]."

Port 60 is normally unassigned. Thus, the above quoted words seem simply to reiterate the idea that using non-standard (e.g., normally unassigned) port numbers for web servers might enhance security. Nothing in the above quoted words teaches or even suggests configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

Ogdon at col. 16 lines 19 to 23 says:

"Note that special security presentation performances can be run using any port number desired when using servers 248 in the operations center, or on intranets (e.g., the secure corporate intranet 260)."

The above quoted sentence simply reiterates the idea that using non-standard port numbers for web servers might enhance security. Nothing in the above quoted words teaches or even suggests configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 (normally assigned to HTTP sessions) rather than port 443 (normally assigned to HTTPS sessions).

The next two sentences cited by the Examiner, Ogdon at col. 16 lines 23 to 32, discuss how the HTTPS protocol can be useful for transmitting questions to participants, collecting responses from participants and returning results to participants. Nothing in those sentences teaches or even suggests configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 (normally assigned to HTTP sessions) rather than port 443 (normally assigned to HTTPS sessions).

Applicant has diligently reviewed the remaining discussion of Ogdon's security subsystem, appearing in Ogdon at col. 16 line 32 to col. 18 line 19. Applicant has been unable to find in those portions of Ogdon anything that teaches or

even suggests configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

Ogdon Conclusion. Thus, for the reasons discussed above, Ogdon alone neither teaches nor suggests configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443, despite the Examiner's assertion to the contrary.

3.1.3. Cianfrocca and Ogdon combined do NOT teach or even suggest configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443. As discussed in detail above, neither Cianfrocca nor Ogdon teaches or even suggests the first element expressly required by claim 3, to wit: configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443. Consequently, even if one should combine copies of both Cianfrocca and Ogdon into a single document, the resulting consolidated document would contain nothing that teaches or even suggests the first element expressly required by claim 3, to wit: configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

3.2. None of Cianfrocca, Ogden, nor Cianfrocca combined with Ogden, teaches or even suggests: receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443.

3.2.1. Cianfrocca alone does NOT teach or even suggest receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443.

In the Office Action at page 3, line 20 and page 3 line 24 to page 4 line 4, the Examiner asserts "... said method comprising: ... (b) receiving at the server program on the second port number a first data packet in a manner that is consistent with the secure hypertext transfer protocol [col. 20, lines 20-32; col. 17, lines 35-40; and col. 15, 28-32],".

As discussed above, it appears that the Examiner believes that port 80 corresponds to the second port number of Claim 3 and that HTTPS corresponds to the secure hypertext transport protocol of Claim 3. Thus, the Office Action at page 3, line 20 and page 3 line 24 to page 4 line 4 is equivalent to an assertion that Cianfrocca at col. 20, lines 20-32, col. 17, lines 35-40 and col. 15, lines 28-32 discloses receiving at the server program on port 80 a first data packet in a manner that is consistent with HTTPS.

However, the portions of Cianfrocca cited above by the Examiner do NOT disclose what the Examiner claims they disclose.

Applicant has carefully examined Cianfrocca at col. 20, lines 20-32 and is unable to find therein any disclosure of (i) receiving on any port a data packet in a manner that is consistent with HTTPS or (ii) receiving on port 80 a data packet in a manner that is consistent with HTTPS.

Cianfrocca at col. 17, lines 35-40 expressly teaches that the server should be configured to listen for requests for secure hypertext transfer protocol sessions on port 443 (NOT port 80 as required by Claim 3).

Applicant has carefully examined Cianfrocca at col. 15, lines 28-32 and is unable to find therein any disclosure of (i) receiving on any port a data packet in a manner that is consistent with HTTPS or (ii) receiving on port 80 a data packet in a manner that is consistent with HTTPS.

Cianfrocca Conclusion. Thus, for the reasons discussed above, Cianfrocca alone neither teaches nor suggests receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443, despite the Examiner's assertion to the contrary.

3.2.2. Ogdon alone does NOT teach or even suggest receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443.

Applicant has examined Ogdon and has been unable to find in Ogdon any teaching or suggestion of this element of Claim 3.

The Office Action contains no assertion that Ogdon teaches or suggests this element of Claim 3.

Ogdon Conclusion. Thus, for the reasons discussed above, Ogdon alone neither teaches nor suggests receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443.

3.2.3. Cianfrocca and Ogdon combined do NOT teach or even suggest receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443. As discussed in detail above, neither Cianfrocca nor Ogdon teaches or even suggests the second element expressly required by claim 3, to wit: receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443. Consequently, even if one should combine copies of both Cianfrocca and Ogdon into a single document, the resulting consolidated document would contain nothing that teaches or even suggests the second element expressly required by claim 3, to wit: receiving at the server program on port 80 a first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request is received on port 80 rather than port 443.

3.3. None of Cianfrocca, Ogdon, nor Cianfrocca combined with Ogden, either teaches or suggests: outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443.

3.3.1. Cianfrocca alone does NOT teach or even suggest outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443.

In the Office Action at page 3, line 20 and page 4 line 24 to page 4 line 4, the Examiner asserts "… said method comprising: … (c) outputting from the server program a response to the first data packet in a manner that is consistent with the

secure hypertext transfer protocol [col. 20, lines 20-32; col. 17, lines 35-40; and col. 15, 28-32]."

However, the portions of Cianfrocca cited above by the Examiner do NOT disclose what the Examiner claims they disclose.

Applicant has carefully examined Cianfrocca at col. 20, lines 20-32 and is unable to find therein any disclosure of outputting a data packet in a manner that is consistent with HTTPS.

Applicant has carefully examined Cianfrocca at col. 17, lines 35-40 and is unable to find therein any disclosure of outputting, in response to a packet received on port 80, a data packet in a manner that is consistent with HTTPS.

Applicant has carefully examined Cianfrocca at col. 15, lines 28-32 and is unable to find therein any disclosure of outputting a data packet in a manner that is consistent with HTTPS.

Cianfrocca Conclusion. Thus, for the reasons discussed above, Cianfrocca alone neither teaches nor suggests outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443, despite the Examiner's assertion to the contrary.

3.3.2. Ogdon alone does NOT teach or even suggest outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443.

Applicant has examined Ogdon and has been unable to find in Ogdon any teaching or suggestion of this element of Claim 3. The Office Action contains no assertion that Ogdon teaches or suggests this element of Claim 3.

Ogdon Conclusion. Thus, for the reasons discussed above, Ogdon alone neither teaches nor suggests outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443.

3.3.3. Cianfrocca and Ogdon combined do NOT teach or even suggest outputting from the server program a response to the first data packet in a manner that is

consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443. As discussed in detail above, neither Cianfrocca nor Ogdon teaches or even suggests the third element expressly required by claim 3, to wit: outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443. Consequently, even if one should combine copies of both Cianfrocca and Ogdon into a single document, the resulting consolidated document would contain nothing that teaches or even suggests the third element expressly required by claim 3, to wit: outputting from the server program a response to the first data packet in a manner that is consistent with the secure hypertext transfer protocol, except that the request was received on port 80 rather than port 443.

3.4. At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a web server would be advised to use a port number other than 80 (the default port for HTTP).

As discussed in the Specification at paragraphs [0232] – [0236], Applicant's invention seeks to solve the following problem (the "Firewall Problem"): how can a client computer use HTTPS to communicate securely with a server computer when such client computer is connected to the Internet through a firewall that (i) blocks packets addressed to destination port 443 (the port number normally associated with HTTPS) but (ii) passes packets addressed to destination port 80.

At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP).

3.4.1. Apache manuals. The materials available at http://ftp.monash.edu.au/pub/ap/Apache/ch01.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch04.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch05.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch07.htm (hereinafter, collectively, "Apache Manual") teach away from using port 80 for any protocol other than http and teach away from using any of ports 1 to 1024 as a nonstandard port for a server.

In Chapter 1 of Apache Manuals at Fig. 1.1 (page 3 of 11 when printed by Applicant), the www service (which uses http, the hyper text transfer protocol) is equated with port 80. This teaches away from the notion that port 80 should be used for other protocols, including without limitation SSL/https.

In Chapter 7 of Apache Manuals under the heading "Protecting Your Data from Outside Access" at "Caution" (which appears on page 29 of 38 when printed by Applicant), in the context of discussing how to hide a non-secure/http server, says in relevant part:

> "The second way to make your server less likely to be found is to run it on a nonstandard port. Ports can range from 0 to 65,535, so there is a wide range to choose from. Generally, the first 1024 are considered reserved ports."

By pointing out how many ports are potentially available and observing that the first 1024 are considered reserved ports, Apache teaches away from moving any server to a non-standard port in the range from 0 to 1024. That range includes port 80 which is normally associated with HTTP / hyper text transfer protocol.

3.4.2. Running a Perfect Web With Windows. Applicant previously filed a copy of Running a Perfect Web Site with Windows – Chapter 5, hereinafter "Windows (Chapter 5)" (from the web at http://www.gsu.unibel.by/pub/perf_web/06r07632.HTM).

The notice at the top of Windows (Chapter 5) says "Copyright © 1996" and is very similar to the notice at the top of Chapter 4 of Apache that was provided by the Examiner.

Windows (Chapter 5) at the bottom of page 3 says in relevant part:

> "… Ports under 1024 are reserved for the most common types of Internet traffic, so it is recommended that you use a number above 1024 if you need an alternate port. …"

3.5. Applicant's invention has unexpected, serendipitous or counter-intuitive results. At the time of Applicant's invention, based upon materials such as Apache Manuals and Windows (Chapter 5), one skilled in the art would have expected that changing the port number on which an HTTPS server listens for session requests would make it harder for clients to communicate with such server. However, for clients

connected to the Internet through certain types of firewalls, configuring an HTTPS server to listen on port 80 can make it easier for a client to establish an HTTPS session with such server. In fact, in circumstances where it would NOT have been possible to establish an HTTPS session with such server if it were listening on port 443, the default port for HTTPS, Applicant's invention makes an HTTPS session with such server possible.

It is unexpected, serendipitous and counter-intuitive that configuring a server to listen to a non-standard and unexpected port makes it easier for some clients to reach such server, since this is precisely the sort of change that Apache and Windows (Chapter 5) teaches will make it harder for browsers to communicate with such server.

The unexpected, serendipitous and counter-intuitive results obtained by practicing Applicant's invention cut strongly against the Examiner's view that Applicant's invention was obvious at the time it was made.

3.6. During the period (the "Post Ogdon Period") from December 12, 2000 (the later of the issue date of Cianfrocca and the issue date of Ogdon) through at least December 13, 2005 (the "Test Date"), a period of just over 5 years, others skilled in the art did NOT regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem (as defined above at 3.4).

3.6.1. General Discussion of the Failure of Others to Re-Invent Applicant's Wheel.

The technical staff of every e-commerce web site that attempted to do business with the general public during the Post Ogdon Period ought eventually to have encountered the Firewall Problem since some customers and some potential customers ought to have spent some time at offices or other locations where their computers were connected to the Internet through firewalls that blocked outgoing packets addressed to destination port 443.

Consequently, if Applicant's invention should have been obvious to anyone skilled in the art who encountered (or continued to face) the Firewall Problem during the Post Ogdon Period, then it would be logical to expect that during the Post Ogdon Period the technical staffs of several e-commerce web sites that sought to do business with the general public would either (i) have duplicated Applicant's invention

(e.g., configured HTTPS servers to listen on port 80 and directed clients browsers to request information using a universal resource locator of the form "https://www.domain.com:80") or (ii) have settled upon some other solution to the Firewall Problem that permits secure communication with affected customers' computers.

However, Applicant is not personally aware of any web sites that during or after the Post Ogdon Period have directed a customer's browser to a resource locator of the form https://www.domain.com:80 or implemented some other solution to the Firewall Problem that permits secure communication with customers' computers that are affected by the Firewall Problem (i.e., connected to the Internet through a firewall that passes outbound packets addressed to port 80 but blocks outbound packets addressed to port 443).

Consider for example the web sites barnesandnoble.com and amazon.com – two popular, highly competitive, technologically savvy e-commerce web sites that seek to conduct business with the general public.

3.6.2. barnesandnoble.com. It appears that when confronted with the Firewall Problem at times through the Test Date, the persons skilled in the art employed by barnesandnoble.com decided to drop back and punt. To ensure security, barnesandnoble.com used SSL (i.e., HTTPS) for order submission and the collection of credit card information. As of the Test Date, if a computer connected to the Internet through a firewall that blocked outgoing packets addressed to destination port 443 was used to attempt to place an order, the barnesandnoble.com web site would allow the user of such computer to fill up a shopping cart but at checkout time the browser on such computer would display an unhelpful error message as soon as the customer's browser was directed to establish an HTTPS session using the default destination port of 443.

3.6.3. amazon.com. Based on tests conducted by Applicant on the Test Date, it is clear that when confronted with the Firewall Problem, the persons skilled in the art employed by amazon.com failed, at all times prior to and including the Test Date, to duplicate Applicant's invention or to implement some different solution that permits encrypted communication with affected customers. On the Test Date, the folks at amazon.com clearly recognized the Firewall Problem, warned customers about it, and

offered affected customers the choice of giving up or submitting order and payment details in an unsecured manner (i.e., using HTTP rather than HTTPS). In particular, on the Test Date, the checkout pages at amazon.com would send to a customer (using unsecure HTTP) a web page that contained both:

a button labeled:

"Sign in using our secure server"

and a link that said:

"The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server."

If on the Test Date a customer should have clicked on the button labeled "Sign in using our secure server", then such customer's browser would have been directed to a URL of the form "https://www.amazon.com/*", which by default implies destination port 443. If such customer's computer should have been connected to the Internet through a firewall that blocked outgoing packets addressed to destination port 443 and such customer should have clicked on such button, then such customer would have seen an uninformative error message.

If on the Test Date a customer should have clicked on the "standard server" link described above, then such customer's browser would have been directed to a URL of the form "http://www.amazon.com/*" which by default implies destination port 80, thereby avoiding part of the Firewall Problem. Unfortunately, since that URL begins with "http", the remainder of the checkout process, including the transmission of credit card information, would have been conducted using HTTP which is NOT encrypted for security.

3.6.4. Conclusion. Since popular e-commerce sites that sought to do business with the general public during the Post Ogdon Period neither (i) routinely used URLs of the form "https://www.securedomain.com/*:80" for the secure portions of their check out procedures nor (ii) routinely use some other solution to the Firewall Problem to permit secure, encrypted communications with affected customers' computers, Applicant contends that Applicant's invention was not obvious when it was first reduced to practice

by Applicant, did not become obvious when Cianfrocca and Ogdon issued, and remains non-obvious today, more than eight (8) years later.

3.7. Ogden teaches away from configuring a web server to use for a first protocol a port that is normally assigned to a second protocol.

Cianfrocca at col. 17, lines 35-38 says "Web browsers accessing the system from outside the DMZ will connect via HTTP/HTTPS on the normal TCP ports for these protocols (80 and 443, respectively)…"

Ogdon at col. 16 lines 14-19, the one place where Applicant found any disclosure by Ogdon of the particular non-standard port numbers that Ogdon prefers to assign to a server, Ogdon says:

> "Also note that the security measures for the present invention are not restricted to providing communications on generally used port numbers (e.g., communication between the host and leaders or audience members can occur on either port 60 or port 80 in any combination for a single presentation performance[])."

Port 60 is unassigned, i.e., it is not generally used for any protocol. Port 80 is normally used for HTTP communications. Thus, where Ogdon might have made the Examiner happy (and Applicant unhappy) by suggesting that one associate HTTP with a port number which is normally associated with some other protocol, Ogdon in fact teaches away from the invention of Claim 3 by suggesting that one seeking security through obscurity ought to associate HTTP with port 60 (which is normally assigned to NO protocol).

3.8. The Examiner has not provided an adequate statement of the basis for the examiner's view that the differences between the subject matter of Claim 3 on the one hand and the disclosure in Cianfrocca and/or Ogden on the other hand, are such that the subject matter of Claim 3 as a whole would have been obvious at the time Applicant's invention was made to a person having ordinary skill in the art to which Claim 3 pertains. Without limiting the generality of the foregoing, the Office Action does not set forth or describe a set of modifications to Cianfrocca (both modifications suggested to the Examiner by Ogdon and other modifications suggested by the Examiner) that both (i) would bring Cianfrocca as so modified within the scope of Claim 3 and (ii) would have

been obvious to one skilled in the art who was aware of Cianfrocca and/or Ogdon. Since the Examiner has failed to provide a statement of the basis, if any, for the Examiner's view as to what one skilled in the art might do, Applicant argues that rejection for obviousness fails due to the absence, in the Office Action, of any reasonable statement as to the basis for the views expressed by the Examiner to provide the elements that are missing in the reference. See *In Re Alhert and Kruger*, 165 USPQ 418 (CCPA 1970). In light of the foregoing, Applicant respectfully requests that Claim 3 be allowed.

Discussion - Claim 10

10. Claim 10 IS patentable over Cianfrocca further in view of Ogden because:

10.1. None of Cianfrocca, Ogden, nor Cianfrocca combined with Ogden, teaches or even suggests: configuring a web server system to use port 80 for communications using a protocol selected from the group consisting of: secure socket layer, secure sockets layer, SSL, secure hypertext transfer protocol, and HTTPS (such a protocol, a "Secure Protocol").

10.1.1. Cianfrocca alone does NOT teach or even suggest configuring a web server system to use port 80 for communications using a Secure Protocol. In the Office action at page 4 line 24 - page 5 line 5, the Examiner asserts that "Cianfrocca et al. disclose a method and system means for: receiving at port 80 at the web server system a first data packet that is formatted in accordance with the protocol [col. 20, lines 20-32; col. 17, lines 35-40; and col. 14, line 57 to col. 15, line 32]; …".

The portions of Cianfrocca cited by the Examiner in support of this assertion do NOT teach what the Examiner says they teach.

Cianfrocca at col. 20, lines 20-32 actually says:

> "The NSAPI/ISAPI gateways provide a mechanism for examining HTTP requests received by conventional Web servers and selectively passing some of the requests to a messenger system for servicing as messenger system enabled requests. The replies, generated by messenger system enabled application components, are routed automatically back through the messenger system, then through the Web server gateway program, back to the conventional Web server and ultimately to the Web browser that generated the original request. In order to accomplish the connectivity to the messenger system, the gateway programs are

normal messenger system enabled application components. They are programs linked with the User Agent library, and they make normal TCP connections to the messenger system."

Applicant has diligently reviewed the lines quoted immediately above and has been unable to find therein any reference to port 80 or to any packet formatted in accordance with a Secure Protocol.

Cianfrocca at col. 17, lines 35-40 actually says:

"Web browsers accessing the system from outside the DMZ will connect via HTTP/HTTPS on the normal TCP ports for these protocols (80 and 443, respectively), so the messenger system must be configured to allow these connections, and to disallow TMSP connections on ports 80 and 443"

Applicant has diligently reviewed the lines quoted immediately above and has been unable to find therein any disclosure of receiving at port 80 a data packet formatted in accordance with a Secure Protocol. In fact, the above quoted lines teach AWAY from the claimed invention by stating that web browsers will connect via HTTP on port 80 and HTTPS on port 443, their normal TCP ports.

Applicant has diligently reviewed Cianfrocca at col. 14, line 57 to col. 15, line 32 and is unable to find therein any disclosure of Secure Protocol communication on any particular port number (443, 80 or other).

Cianfrocca Conclusion. Thus, for the reasons discussed above, Cianfrocca alone neither teaches nor suggests configuring a web server system to use port 80 for communications using a Secure Protocol.

10.1.2. Ogdon alone does NOT teach or even suggest configuring a web server system to use port 80 for communications using a Secure Protocol. In the Office action at page 5 lines 14-18, the Examiner asserts that "Ogdon teaches the port 80 is used for communication with the server using the secure hypertext transfer protocol, which is one of various protocols selected from the group consisting of: secure socket layer, secure sockets layer, SSL, secure hypertext transfer protocol, and HTTPS [col. 16 lines 14-31]".

Applicant finds this assertion by the Examiner particularly confusing. It is essentially the same as the assertion that the Examiner made in the Office Action mailed August 21, 2007at page 3 lines 7-9. That assertion was the subject of

Paragraph 10.1.2 of the Appeal Brief filed on 09/22/2008. In the current Office Action at page 2, lines 4-9, the Examiner said he was persuaded by Applicant's argument in the Appeal Brief filed on 09/22/2008 that Ogdon does NOT teach or even suggest configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on port 80 rather than port 443.

Applicant is at a loss to understand how the Examiner went from persuaded to un-persuaded within 3 double spaced pages.

See the detailed discussion above at 3.1.2.

10.1.3. Cianfrocca and Ogdon combined do NOT teach or even suggest configuring a web server system to use port 80 for communications using a Secure Protocol. As discussed in detail above, neither Cianfrocca nor Ogdon teaches or even suggests the first element expressly required by Claim 10, to wit: configuring a web server system to use port 80 for communications using a Secure Protocol. Consequently, even if one should combine copies of both Cianfrocca and Ogdon into a single document, the resulting consolidated document would contain nothing that teaches or even suggests the first element expressly required by Claim 10, to wit: configuring a web server system to use port 80 for communications using a Secure Protocol.

10.2. None of Cianfrocca, Ogden, nor Cianfrocca combined with Ogden, teaches or even suggests: receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol.

10.2.1. Cianfrocca alone does NOT teach or even suggest receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.1.1.

10.2.2. Ogdon alone does NOT teach or even suggest receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.1.2.

10.2.3. Cianfrocca and Ogdon combined do NOT teach or even suggest receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol. As discussed in detail above, neither Cianfrocca nor Ogdon teaches or even suggests the second element expressly required by Claim 10, to wit: receiving at port 80 at the web server system a first data packet that is formatted in

accordance with the Secure Protocol. Consequently, even if one should combine copies of both Cianfrocca and Ogdon into a single document, the resulting consolidated document would contain nothing that teaches or even suggests the second element expressly required by Claim 10, to wit: receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol.

10.3. None of Cianfrocca, Ogdon, nor Cianfrocca combined with Ogden, either teaches or suggests: responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol.

10.3.1. Cianfrocca alone does NOT teach or even suggest responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. In the Office action at page 5 lines 6-8 the Examiner asserts that "responding to the first data packet with a second data packet that is formatted in accordance with the protocol [col. 20, lines 20-32; col. 17, lines 35-40; and col. 14, line 57 to col 15, line 32]." However, the portions of Cianfrocca cited by the Examiner to support this assertion do not teach what the Examiner says they teach. See the detailed discussion above at 10.1.1 and consider the following:

Applicant has diligently examined Cianfrocca at col. 20, lines 20-32 and has been unable to find therein any disclosure of any data packets formatted in accordance with any Secure Protocol.

Cianfrocca at Col. 17, lines 35-40 teaches away from this element of Claim 3 by teaching that web browsers access the system via HTTP on port 80 and HTTPS on port 443. This implies that any response in HTTPS format is to be made in response to a packet received at port 443 (NOT port 80).

Applicant has diligently examined Cianfrocca at col. 14, line 57 to col 15, line 32 and has been unable to find therein any disclosure of responding in HTTPS format to a packet received on port 80.

10.3.2. Ogdon alone does NOT teach or even suggest responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. In the Office action at page 5 lines 14-18 the Examiner asserts that "Ogdon teaches the port 80 is used for communication with the server using the secure hypertext transfer protocol, which is one of various protocols selected from the group consisting of:

secure socket layer, secure sockets layer, SSL, secure hypertext transfer protocol, and HTTPS [col. 16 lines 14-31]". . However, the portions of Cianfrocca cited by the Examiner to support this assertion do not teach what the Examiner says they teach. See the detailed discussion above at 10.1.2.

10.3.3. Cianfrocca and Ogdon combined do NOT teach or even suggest responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. As discussed in detail above, neither Cianfrocca nor Ogdon teaches or even suggests the third element expressly required by Claim 10, to wit: responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. Consequently, even if one should combine copies of both Cianfrocca and Ogdon into a single document, the resulting consolidated document would contain nothing that teaches or even suggests the third element expressly required by Claim 10, to wit: responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol.

10.4. At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a web server would be advised to use a port number other than 80 (the default port for HTTP). See the detailed discussion of this point above at 3.4.

10.5. Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the detailed discussion of this point above at 3.5.

10.6. During the Post Ogdon Period (from December 12, 2000 through at least December 13, 2005), a period of just over 5 years, others skilled in the art did NOT regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem (as defined above at 3.4). See the detailed discussion above at 3.6.

10.7. Ogden teaches away from configuring a web server to use for a first protocol a port that is normally assigned to a second protocol. See the detailed discussion above at 3.7.

10.8. The Examiner has not provided an adequate statement of the basis for the examiner's view that the differences between the subject matter of Claim 10 on the one hand and the disclosure in Cianfrocca and/or Ogden on the other hand, are such that the subject matter of Claim 10 as a whole would have been obvious at the time Applicant's

invention was made to a person having ordinary skill in the art to which Claim 10 pertains. Without limiting the generality of the foregoing, the Office Action does not set forth or describe a set of modifications to Cianfrocca (both modifications suggested to the Examiner by Ogdon and other modifications suggested by the Examiner) that both (i) would bring Cianfrocca as so modified within the scope of Claim 10 and (ii) would have been obvious to one skilled in the art who was aware of Cianfrocca and/or Ogdon. Since the Examiner has failed to provide a statement of the basis, if any, for the Examiner's view as to what one skilled in the art might do, Applicant argues that rejection for obviousness fails due to the absence, in the Office Action, of any reasonable statement as to the basis for the views expressed by the Examiner to provide the elements that are missing in the reference. See *In Re Alhert and Kruger*, 165 USPQ 418 (CCPA 1970). In light of the foregoing, Applicant respectfully requests that Claim 10 be allowed.

Discussion - Claim 11

11. Claim 11 IS patentable over Cianfrocca further in view of Ogden because:

11.1. None of Cianfrocca, Ogden, nor Cianfrocca combined with Ogden, teaches or even suggests: web server software configured to use port 80 for communications using a Secure Protocol.

11.1.1. Cianfrocca alone does NOT teach or even suggest web server software configured to use port 80 for communications using a Secure Protocol. See the detailed discussion above at 10.1.1.

11.1.2. Ogdon alone does NOT teach or even suggest web server software configured to use port 80 for communications using a Secure Protocol. See the detailed discussion above at 10.1.2.

11.1.3. Cianfrocca and Ogdon combined do NOT teach or even suggest web server software configured to use port 80 for communications using a Secure Protocol. See the detailed discussion above at 10.1.3.

11.2. None of Cianfrocca, Ogden, nor Cianfrocca combined with Ogden, teaches or even suggests: a means for receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol.

11.2.1. Cianfrocca alone does NOT teach or even suggest a means for receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.2.1.

11.2.2. Ogdon alone does NOT teach or even suggest a means for receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.2.2.

11.2.3. Cianfrocca and Ogdon combined do NOT teach or even suggest a means for receiving at port 80 at the web server system a first data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.2.3.

11.3. None of Cianfrocca, Ogdon, nor Cianfrocca combined with Ogden, either teaches or suggests: a means for responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol.

11.3.1. Cianfrocca alone does NOT teach or even suggest a means for responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.3.1.

11.3.2. Ogdon alone does NOT teach or even suggest a means for responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.3.2.

11.3.3. Cianfrocca and Ogdon combined do NOT teach or even suggest a means for responding to the first data packet with a second data packet that is formatted in accordance with the Secure Protocol. See the detailed discussion above at 10.3.3.

11.4. At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a web server would be advised to use a port number other than 80 (the default port for HTTP). See the detailed discussion of this point above at 3.4.

11.5. Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the detailed discussion of this point above at 3.5.

11.6. During the Post Ogdon Period (from December 12, 2000 through at least December 13, 2005), a period of just over 5 years, others skilled in the art did NOT

regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem (as defined above at 3.4). See the detailed discussion above at 3.6.

11.7. Ogden teaches away from configuring a web server to use for a first protocol a port that is normally assigned to a second protocol. See the detailed discussion above at 3.7.

11.8. The Examiner has not provided an adequate statement of the basis for the examiner's view that the differences between the subject matter of Claim 11 on the one hand and the disclosure in Cianfrocca and/or Ogden on the other hand, are such that the subject matter of Claim 11 as a whole would have been obvious at the time Applicant's invention was made to a person having ordinary skill in the art to which Claim 11 pertains. Without limiting the generality of the foregoing, the Office Action does not set forth or describe a set of modifications to Cianfrocca (both modifications suggested to the Examiner by Ogdon and other modifications suggested by the Examiner) that both (i) would bring Cianfrocca as so modified within the scope of Claim 11 and (ii) would have been obvious to one skilled in the art who was aware of Cianfrocca and/or Ogdon. Since the Examiner has failed to provide a statement of the basis, if any, for the Examiner's view as to what one skilled in the art might do, Applicant argues that rejection for obviousness fails due to the absence, in the Office Action, of any reasonable statement as to the basis for the views expressed by the Examiner to provide the elements that are missing in the reference. See *In Re Alhert and Kruger*, 165 USPQ 418 (CCPA 1970). In light of the foregoing, Applicant respectfully requests that Claim 11 be allowed.

In light of the foregoing, Applicant respectfully requests that Claims 3, 10 and 11 be allowed.

Respectfully,

/s/

Carl Oppedahl
PTO Reg. No. 32,746